AGENCY OF HUMAN SERVICES

# AHS Maintenance Standard

**Jack Green**

**10/9/2013**

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the Maintenance ( MA-1, MA-2, MA-2(1), MA-3, MA-3(1), MA-3(2), MA-4, MA-4(1), MA-4(2), MA-4(3), MA-5, MA-6) Controls.

# Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| | .99 | Procedures received from HI and reviewed by Referentia | |
| 10/9/2013 | 3.0 | Procedures reviewed and adapted for VHC business processes and security requirements | Jack Green |

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the Maintenance (MA-1, MA-2, MA-2(1), MA-3, MA-3(1), MA-3(2), MA-4, MA-4(1), MA-4(2), MA-4(3), MA-5, MA-6) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

**Controlled Maintenance**

1. The VHC shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.
2. Maintenance and repairs on information system components are scheduled and performed in accordance with manufacturer or vendor specifications and/or VHC requirements.
    - The maintenance schedule and procedures must be documented in a Maintenance Plan.
        - The Maintenance Plan must address how the maintenance schedule is managed and the Point of Contact (POC) for scheduled maintenance.
    - Scheduled maintenance must include controls to monitor the completion of maintenance in accordance with the information system's documented maintenance schedule and vendor recommendations.
    - Maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.
    - The VHC shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.

- The VHC shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.
- The VHC shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.
- If a manufacturer, vendor, or developer provided maintenance schedule does not exist, the system must be reviewed every three months in order to determine if maintenance is required.
- Any maintenance action that must be performed outside of the scheduled maintenance timeframes must adhere to the information system's documented procedures for unscheduled maintenance.

3. The VHC ensures that all maintenance and repair activities, including non-local maintenance and diagnostics, are documented
4. All maintenance records are reviewed and confirmed monthly.
5. All maintenance activities must be controlled under all circumstances:
    - Whether performed on site or remotely.
        a. If performed remotely, the actual maintenance itself must be performed within a VHC Office.
        b. In the event the maintenance planning does not include performing remote maintenance, the VHC will disable all remote maintenance capabilities.
    - Whether the equipment is serviced on site or removed to another location.
    - When FTI data may be accessible during maintenance, the maintenance must be performed in the presence of authorized VHC personnel.
6. Any system or media that has FTI data on it and is being removed to another location will have all FTI destroyed prior to the system or media being removed.
    - An IRS approved destruction method must be used.
7. Notification must be provided to all impacted users informing them of scheduled, unscheduled, and emergency maintenance on the information system.
    - Email notification is preferable for external users.
    - Notification via the web for external users must consider the extent of information and detail of information disclosed.
        - For example, providing the precise name of servers in the notification may provide information for social engineering threats.
    - Help desk personnel must be notified and reminded not to provide unauthorized information unless the identity of the user can be confirmed.
    - The following must be addressed in the notification.
        - The expected start and finish time of the maintenance.
        - The purpose of the maintenance activity.

        - The specific information systems or subcomponents that may be impacted by the maintenance.
        - Any actions required of the impacted users in coordination with the maintenance effort.
        - Contact information should a user have any questions or concerns related to the maintenance effort.
    - An updated notification must be sent should the expected start or finish time or any other parameter of the maintenance change.
    - The System Owner (SO) and the party that requested the maintenance, if applicable, must be notified when maintenance is completed.
    - Following maintenance or repair actions, the security features must be checked to verify that they are still functioning properly.

**Maintenance Tools**

1. The use of information system maintenance tools must be approved, controlled, and monitored.
2. Use of the approved maintenance tool must be defined and documented in the Maintenance Plan.
    i. If a tool is needed (e.g., in emergency maintenance situations) and the tool is not listed in the Maintenance Plan, written approval must be given by the System Owner.
    ii. The Security Officer's written approval must then be included as an attachment to the Maintenance Plan after the fact.
    iii. Once the maintenance is completed, one of the following actions is required:
        a. The tool must be formally documented and added to the list in the Maintenance Plan.
        b. The tool must be removed from the information system and no longer used.
3. All media containing diagnostic and test programs (e.g., software or firmware used for system maintenance or diagnostics) must be checked for malicious code before the media are used in the information system.
4. All approved tools must be maintained on an ongoing basis.
    i. A maintenance schedule must include the maintenance of the information system's maintenance tools and the schedule must be documented in the Maintenance Plan.
    ii. Maintenance tools must receive vendor recommended maintenance, and the maintenance must be documented with other information system maintenance records.
    iii. If maintenance tools are supported by vendor or third party agreements, the agreements must include SLAs appropriate for the information system.

**Non-Local Maintenance**

1. Non-local maintenance and diagnostic activities performed on the information system must be authorized, logged, monitored, and controlled.
2. The use of non-local maintenance and diagnostic tools must be consistent with VHC policy and requirements and documented in the information system's SSP.
    i. Non-locally executed maintenance and diagnostic activities must not bypass information technology security controls or violate VHC policy or requirements.
3. Strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions must be employed.
4. Identification and authentication techniques must be consistent with the network access requirements found in the Identification and Authentication Procedures (IA1).
5. Maintenance records must be maintained for all non-local maintenance, diagnostic, and service activities.
6. Refer to the Controlled Maintenance section of this procedure document for VHC standards on the components of all maintenance records.
7. Access information such as passwords or port information must be communicated out of band by secure means (e.g., encrypted communications, phone).
8. When non-local maintenance and diagnostic activities are completed, the following must be adhered to and verified:
    i. All sessions and network connections invoked in the performance of the activity must be terminated.
    ii. All temporarily enabled or opened maintenance ports, services, or protocols must be disabled or closed again.
    iii. All temporary access must be disabled.

**Maintenance Personnel**

1. A process for maintenance personnel authorization must be established.
2. Only authorized personnel shall perform maintenance on the information system.
3. A current list of authorized maintenance organizations or personnel must be maintained.
4. Personnel performing maintenance on the information system must have the required access authorizations.
    i. When maintenance personnel do not possess the required access authorizations, VHC personnel with the required access authorizations and technical competence deemed necessary must be designated to supervise information system maintenance.
    ii. Maintenance personnel who do not possess the required access authorizations must be escorted at all times while performing information system maintenance at the VHC or on any VHC site.

5. Before accessing a VHC information system, all third-party maintenance personnel must have:
    i. Individually signed a non-disclosure form.
    ii. Provided valid identification.
6. Personnel who are to perform routine maintenance must be both expected (i.e., there must be a schedule or notification) and pre-approved.
    i. When emergency maintenance is needed, the personnel must still be preapproved.

**Timely Maintenance**

1. Timely maintenance provisions (i.e., SLAs or equivalent language) must be included in all maintenance agreements for the information system.
    i. The timely maintenance provisions must cover maintenance support and/or spare or replacement parts for both routine maintenance and when there are failures, emergencies, or a need for unscheduled maintenance.
    ii. The timely maintenance provisions must be expressed in terms of the timeframe from notification of the failure, emergency, or need for unscheduled maintenance.
    iii. The provisions must address the timeframe for dispatching technicians.
2. The maintenance agreements must define the security-critical information system components and/or key information technology components for which spare parts or replacement parts must be made available.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec